Evidence Theory-Based Trust Management for the Social Internet of Vehicles

Nasrin Shamaeian
School of Computer Science and IT
University College Cork
Cork, Ireland
n.shamaeian@cs.ucc.ie

Dirk Pesch
School of Computer Science and IT
University College Cork
Cork, Ireland
dirk.pesch@ucc.ie

***Abstract*—The Social Internet of Vehicles (SIoV) is a concept combining the principles of vehicular and social networks, where entities, such as vehicles, drivers, passengers and infrastructure, share information not only for intelligent transportation or cooperative mobility needs, but also using social network principles. Trust in the information exchanged between vehicles in a vehicular network is paramount to achieving safety and reliability of transportation. We propose a trust management model for SIoV that integrates entity trust from direct interactions between vehicles, indirect trust from recommendations, and social trust reflecting the drivers' social attributes. We utilize Dempster–Shafer Theory to effectively manage inherent uncertainties within this network, enabling robust aggregation of various trust evidences. Our simulation results show the effectiveness of our model in accurately identifying and mitigating malicious entities within the network performing trust-related attacks.**

***Index Terms*—Trust management, Internet of Vehicles, Social IoV, Dempster-Shafer theory**

I. Introduction

The Internet of Vehicles (IoV) represents an evolutionary leap in connected transportation, creating a dynamic network where vehicles interact with each other, other traffic participants, and infrastructure. This interconnected environment not only enhances operational efficiency but also raises safety standards throughout transportation systems. Drawing from the foundational concepts of Vehicular Ad-hoc Networks (VANETs), the IoV extends these capabilities, enabling vehicles to become integral components of the broader Internet of Things (IoT) ecosystem [1].

Building on the IoV concept, the Social Internet of Vehicles (SIoV) integrates the social networking paradigm with vehicular networks. The SIoV leverages social interactions among drivers to foster a more interactive and engaging driving experience, supporting a range of applications from safety alerts to traffic and entertainment updates [2]. This integration facilitates improved information exchange and also enhances the communal aspects of travel, turning solitary drives into socially connected experiences. However, the increase in the SIoV brings security issues such as malicious vehicles, false information, selfish behaviours, and transmission delays [3]. Therefore, effective vehicle trust management and control are essential for providing safe and reliable transportation.

Trust management addresses the unique challenges posed by the dynamic and ephemeral nature of vehicular networks. In this context, trust is defined as the confidence a vehicle has that messages sent by other vehicles are reliable, trustworthy, accurate, and authentic [1]. Given that human behaviour significantly influences driving behaviour and thus vehicular communication, trust management in SIoV evaluates the trustworthiness of both vehicles and drivers. For instance, trust is essential when vehicles near a school gate exchange information about students leaving school or parking availability. This exchange relies on the location or proximity of the vehicles and also on the communal trust and relationships established between their drivers. Similarly, on highways, the sharing of details about toll stations or traffic signs depends on the mutual trust between not only vehicles but also drivers that often comes from shared interests or common routes [3].

Trust models are typically categorized into entity-centric, data-centric, and combined models, based on the targets of revocation. Most approaches rely on past interactions or the quality of the exchanged data between vehicular nodes to assess the trustworthiness of vehicles, while the social characteristics of drivers are largely overlooked. The concept of social trust introduces a human-centric dimension to trust management in IoV, reflecting socially aware networking paradigms where human behaviour and relationships influence network dynamics. In SIoV, trust establishment is vital for secure Vehicle-to-Vehicle (V2V) communications, but also for integrating social behaviours of drivers into the network's trust models. This integration acknowledges that the movements and interactions of vehicles are inherently linked to their drivers' social patterns, thereby aligning the trust assessments more closely with human-centric factors. By focusing on these human aspects, the SIoV aims to create a more relatable and efficient network, where trust is built on shared social experiences and the reliability of interactions, enhancing both the security and functionality of vehicular communications.

By combining network-based interactions with the social behaviour of drivers, we propose an entity- and social-centric trust management model for SIoV. Our main contribution is a novel trust management model that uses the Dempster-Shafer

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) under Grant Number 13/RC/2077_P2 (CONNECT Centre for Future Networks)

Theory (DST) combination rule for indirect trust calculations in a vehicular network to account for the inherent uncertainty of this network, combining recommendations leveraging social trust to incorporate similarities between users as a weight factor. These similarities are calculated via a social trust model which evaluates relationships between users in terms of friendship, social contact, and community of interest. We determine our model's performance in detecting trustworthy nodes under common trust-related attacks that can compromise the integrity of reputation systems. We also provide a performance comparison to the weighted sum method and show that our proposed approach presents an improvement in performance when detecting trust-related attacks.

II. Related Work

In the IoV, trust management is categorized into three approaches: entity-based, data-based, and hybrid. Entity-based trust [4] [5] assesses the trustworthiness of network nodes by evaluating their reputations and past behaviours, considering factors like similarity and proximity to enhance trust evaluations. Data-based approaches [6] focus on the authenticity and utility of the data exchanged, using metrics such as event type and vehicular node roles to determine trust. Hybrid approaches combine both entity reputations and data authenticity [7].

A trust inference model to enhance routing security in VANETs is developed in [4]. A method for calculating trust is introduced combining subjective trust derived from historical interactions and recommendation trust calculated using a weighted average of recommendations from multiple recommenders. A trust model for Vehicle-to-Everything (V2X) communication systems is presented in [5] to address internal security threats. In this model, trust is computed using direct and indirect trust components. Direct trust is calculated from a node's past interactions, while indirect trust is based on a weighted average of the feedback from other nodes, combining positive and negative recommendations using a weighted sum. A reputation system for 5G vehicular networks is introduced in [8], where a trusted authority (TA) assigns scores to vehicles based on past behaviour. Vehicles with scores below a set threshold are barred from network communication. This centralized trust model, managed solely by the TA, involves collecting feedback, computing reputation scores, and regulating network access. However, centralized systems are vulnerable to attacks if the TA is compromised. Li et al. [9] present an effective hybrid trust model for VANETs that is resistant to attacks, assessing trust based on both node behaviour and data accuracy. This model evaluates the trustworthiness of received information by analyzing the reliability of the nodes as well as the integrity of the data they provide. Ahmad et al. [1] proposed a hybrid trust assessment framework for IoV that conducts entity verification at the transport layer and data verification at the application layer.

Beyond the entity- or data-based models, there are many trust assessment frameworks that also consider the social aspects of human behaviour. The TACASHI framework for SIoV [2] evaluates vehicle trust by integrating direct trust from the direct interactions of vehicles, and indirect trust considering opinions from other vehicles and roadside units. Social trust is measured by assessing the honesty of users through their online social network profiles. The social trust approach in [10] is primarily based on the social nature of the network formed by vehicles, rather than focusing on individual user characteristics. In the proposed trust framework, vehicles interact with each other within a vehicular social network, exchanging data and forming trust relationships based on these interactions. A trust-aware model is proposed in [3] to enhance the quality of service and content distribution within the SIoV. The model integrates entity trust and social trust. The latter is used to assess individuals' ability to participate in the network's content distribution functions. The trust management solution we have proposed combines components of social trust and entity-based trust. Our novelty lies in the fact that we use the Dempster-Shafer Theory combination rule in order to factor the user's social relationships as a measure of their reputation when performing indirect trust calculations.

III. System Model

A. Preliminaries

We consider a user-centric IoV environment with a set of vehicles V and a set of users U participating in the environment. All vehicles and users are registered with a trusted authority, ensuring each has a unique Public Key. The vehicles are equipped with standard wireless communication interfaces such as ITS-G5 or cellular-V2X, facilitating seamless V2V and Vehicle-to-Infrastructure communications. We define a vehicular network where each node ($\pi \in \Pi \subseteq U \times V$) in the network is a tuple matching a single user with a single vehicle such that ($\pi = \{u, v\}$). A user can be paired with more than one vehicle ($N_v \geq N_u$).

B. Adversary Model

The decentralized and open architecture of the IoV provides adversaries with opportunities to infiltrate the network, exploiting its structure to carry out malicious activities. Their main objectives include intercepting or altering data, and misrepresenting vehicles or users by submitting fraudulent recommendations [1]. We consider trust-related attacks that can compromise the integrity of reputation systems. These attacks disrupt accurate trust evaluations, making it challenging to identify and address actual threats. Below are the primary types of reputation attacks [11] a malicious node can carry out:

- Bad-mouthing Attack: A malicious node disseminates false information during message exchanges, damaging the reputation of well-behaved nodes by spreading negative or false recommendations against them.
- Ballot-stuffing Attack: This attack enhances the reputation of a malicious node through positive, yet falsified, endorsements.
- On-off Attack: A malicious node alternates its behaviour unpredictably between sending incorrect information and seemingly legitimate recommendations.

IV. Trust Framework

A. Modeling Trust

The trustworthiness of a node is represented in subjective logic as an opinion in the form of a tuple of belief b, disbelief d, and uncertainty u [12]. The trust of node i in node j ($T_{i,j}$) is assessed through the combination of direct user satisfaction, or *direct trust* ($T^D_{i,j}$), from previous interactions, and recommendations from other users, also known as *indirect trust* ($T^{ID}_{i,j}$). Indirect trust takes into account the social similarities of users by selecting trust feedback from nodes sharing similar social interests. The management of these social similarities is referred to as *social trust* ($T^S_{i,j}$). We define the frame of discernment as $\Theta = \{T, \overline{T}\}$ [13]. The degree of belief in a node's trustworthiness corresponds to the belief function in Dempster-Shafer Theory as $Bel(T) = m(T) = b$ and the plausibility function as $Pl(T) = 1 - Bel(\overline{T}) = 1 - d$, representing the lower bound and the upper bound of the trust interval respectively.

B. Direct Trust

In our trust model, a node can evaluate another node based on its message content after direct communication. We assume that vehicles send messages in the context of safety alerts, blind spots, intersection collision avoidance, emergency signals, and sensed data. During each interaction, we assume the sender node transmits a message which reflects its behaviour, and the receiver node then evaluates this message. The evaluation produces evidence as an opinion that translates to the degree of belief towards the trustworthiness of the sender. This evaluation considers both the sensing data from the receiver node and the attributes of the message received.

To model this evaluation process, we characterize the first-hand observation of the received message using a normal distribution $\mathcal{N}(\mu, \sigma^2)$ as it allows for more realistic representation of the variability and uncertainty inherent in the evaluation, capturing a wide range of potential observations around a mean value with a given standard deviation. The means μ_b, μ_d, and μ_u represent the belief, disbelief, and uncertainty in the trustworthiness of a node's behaviour, respectively. This method provides a more nuanced and continuous assessment of evidence compared to a binary evaluation.

The direct trust calculation incorporates cumulative scores from the direct interactions and it is subject to decay over time (decay factor ϕ). We use an event-driven approach to update trust dynamically, ensuring that the cumulative trust score is both current and reflective of recent interactions. We consider an exponential decay on the cumulative scores. Here, Δt is the time between interactions. The opinion produced by the receiver is denoted as the tuple of g, m and n.

$$\begin{aligned} \alpha_t &= e^{-\phi \Delta t}\alpha_{t-1} + g \\ \beta_t &= e^{-\phi \Delta t}\beta_{t-1} + m \\ \gamma_t &= e^{-\phi \Delta t}\gamma_{t-1} + n \end{aligned} \tag{1}$$

The direct trust of node i in node j ($T^D_{i,j}$) is calculated into belief, disbelief and uncertainty as:

$$\begin{aligned} b &= \frac{\alpha}{\alpha + \beta + \gamma} \\ d &= \frac{\beta}{\alpha + \beta + \gamma} \\ u &= \frac{\gamma}{\alpha + \beta + \gamma} \end{aligned} \tag{2}$$

C. Social Trust

We employ the design principle of distributed collaborative filtering to select trust feedback from nodes that share similar social interests [14]. We define social trust as the degree of social similarity between users considering three types of social traits of drivers: friendship, social contact, and Community of Interest (CoI). These social relationships are represented by three distinct lists: a list of current friends representing friendships, a list of commonly visited locations representing social contacts indicative of physical proximity, and a list of directly interacted nodes that constitute the CoI indicating similar social interests through membership in the same communities. We assume that the social relationship lists of every user are stored in the On-Board Unit (OBU) of their vehicle and are exchanged during node interactions. We calculate the social similarity measures based on the cosine similarity metric between social lists of users as follows [11]:

Friendship similarity: Defining the vector of friends F_i of U_i and F_j of U_j, we measure the similarity between two nodes by calculating the cosine of the angle between their respective vectors.

$$\text{sim}_f(u_i, u_j) = \frac{\vec{VF}_i \cdot \vec{VF}_j}{\|\vec{VF}_i\| \|\vec{VF}_j\|} = \frac{|F_i \cap F_j|}{\sqrt{|F_i| \cdot |F_j|}} \tag{3}$$

Social contact similarity: The social contact similarity reflects proximity and serves as an indicator of whether two nodes share the same physical interactions. Similar to the friendship similarity we can measure the social contact similarity after the exchange of their location lists L_i and L_j

$$\text{sim}_l(u_i, u_j) = \frac{|L_i \cap L_j|}{\sqrt{|L_i| \cdot |L_j|}} \tag{4}$$

Community of Interest similarity: Two users within the same CoI are likely to have shared social interests, knowledge and standards. Given lists (vectors) C_i and C_j of the interacting vehicles of user i and j, respectively, the CoI similarity is

$$\text{sim}_c(u_i, u_j) = \frac{|C_i \cap C_j|}{\sqrt{|C_i| \cdot |C_j|}} \tag{5}$$

The social similarity between two users is calculated as a weighted combination of all social similarity metrics where $\omega_f + \omega_l + \omega_c = 1$ and $0 \leq \omega_f, \omega_l, \omega_c \leq 1$

$$\text{sim}(u_i, u_j) = \sum_{v \in \{f,l,c\}} \omega_v \cdot \text{sim}_v(u_i, u_x) \tag{6}$$

The belief one user has in another in the context of social trust corresponds directly to their social similarity, with an

inherent uncertainty factor of $1 - \text{sim}$, reflecting the degree of dissimilarity. We calculate the social trust $T^S_{i,j}$ of U_i in U_j as:

$$T^S_{ij} = (\text{sim}(u_i, u_j), 0, 1 - \text{sim}(u_i, u_j)) \tag{7}$$

D. Indirect Trust

In the IoV, indirect trust is a vital metric due to the often sporadic and transient interactions between vehicles. The system's model is influenced by social trust, allowing vehicles to select trust feedback from nodes with similar social interests. Recommendations are considered more trustworthy if the recommender shares a high degree of social trust with the node that is seeking advice. We use the DST combination rule for indirect trust calculation, integrating direct trust towards recommenders with social trust as a weight factor. We use DST for its strong theoretical foundation and well-defined rules for combining evidence from diverse sources with varying reliability and context. DST effectively handles uncertainty and conflict, enabling a principled integration of information and providing a comprehensive trust assessment despite differing reliability of recommenders. The recommendation trust is calculated using the following steps: (1) Direct trust: Each node i computes direct trust $T^D_{i,z}$ based on their experiences with another node z; (2) Social trust calculation: Node i calculates social similarity by measuring the social trust $T^S_{i,z}$ it has in all other nodes z that are within close proximity δ, based on shared social characteristics defined in the previous section; (3) Selecting top k similar users: Node i selects the k nodes with the highest social trust scores as their reference group for recommendations; and (4) Applying DST combination rule: Node i applies the DST combination rule to integrate trust recommendations about node j from the top k socially similar nodes z. The indirect trust from i towards j through each recommender z is computed as:

$$T^{ID}_{i,j} = \bigoplus_{z=1}^{k} \left(T^D_{i,z} \otimes T^S_{i,z} \otimes T^D_{z,j}\right) \tag{8}$$

where $\bigoplus$ denotes the DST rule of belief fusion of the k recommendations, $\otimes$ is the discounting operation used to compute transitive trust, and $T^D_{z,j}$ is the direct trust the recommender z has in vehicle j. This method ensures that the recommendation assessment is predominantly influenced by those users who share strong social ties, leading to a more accurate and socially relevant trust evaluation in an IoV compared to treating all users the same.

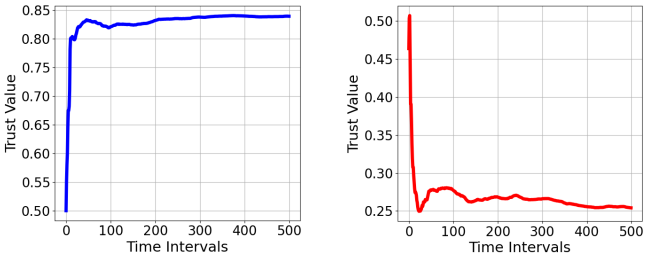
E. Overall Trust

The overall trust of node i in node j ($T_{i,j}$) is derived from the combination of first-hand observations (i.e., Direct Trust) and second-hand observations (i.e., Indirect Trust) as follows:

$$T_{i,j} = T^D_{i,j} \oplus T^{ID}_{i,j} \tag{9}$$

V. Performance Evaluation

In this section, we outline the setup of our simulation and describe the performance metrics we used.



(a) well-behaved node (b) malicious node

Fig. 1: Trust values over time intervals (a) well-behaved node and (b) malicious node

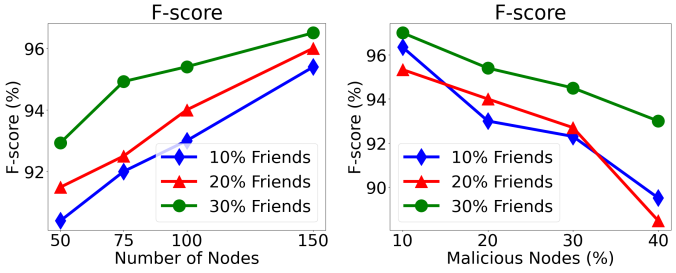
A. Simulation Setup

Our simulation framework is implemented in Python and simulates an environment consisting of N_v vehicles and N_u users ($N_v = N_u$), where vehicles are randomly assigned to users within a given area. To simulate vehicle mobility, we use the SWIM mobility model [15], which is a well-known method for simulating social behaviour patterns among nodes. The mobility pattern of nodes in SWIM is rooted in a basic understanding of human movement: individuals tend to visit locations close to their homes and where there are opportunities to interact with other people in their social circle. This setup aims to capture the realistic social dynamics that can influence node behaviour in a network. Nodes have a defined effective interaction range of $\delta = 50m$, i.e.: nodes within this distance from each other are allowed to communicate. The probability of interaction for two nodes within the effective interaction range is sampled from an exponential distribution with parameter $\lambda = 1/3$.

The decay factor for updating trust is $\phi = 0.001$. The weights for friendship, social contact, and CoI similarities are defined as $\omega_f = 1/2$, $\omega_l = 1/4$, and $\omega_c = 1/4$, respectively. We prioritize friendship similarities with a higher weight within the scope of this work. The evidence values produced from a node's evaluation of a direct interaction were sampled from normal distributions with mean values of $\mu_b = 0.7$, $\mu_d = 0.3$, $\mu_u = 0.1$ for the b, d, u parameters and with $\sigma = 0.1$ as the standard deviation in all cases. These values have been determined through a process of gradient descent.

To ensure variability and robustness, each simulation scenario is executed 100 times, with different random seeds, defining a unique initial placement of nodes across the network. Each simulation is executed until it reaches a sufficient steady state with an estimated trust value converging to the ground truth value. The experimental results for every scenario are averaged over 100 runs using the batch means method to enhance statistical reliability.

In order to model untrustworthy behaviours, nodes are designated as malicious or trustworthy at the beginning of each run based on a Bernoulli distribution with probability p_m. The trustworthiness of a node n_i is measured by its behaviour $B_i \in \{0, 1\}; B_i \sim Bernoulli(p_m)$. A good node follows the



(a) (b)

Fig. 2: F-Score showing effect of (a) node density vs. number of friends (b) number of friends vs. number of malicious nodes

execution of the trust framework honestly, while a malicious node gives false recommendations and sends false information by performing either ballot-stuffing, bad-mouthing, or on-off attacks as described in section III-B.

B. Performance Metrics

To assess the accuracy of our model in identifying trustworthy nodes, we use precision, recall, and F-score as key performance metrics. The performance metrics are defined based on the following parameters: True Positives (TP), which represent the number of nodes correctly identified as malicious by the framework; False Positives (FP), which are the nodes labelled as malicious despite being honest; and False Negatives (FN), which are the malicious nodes detected as honest.

VI. Simulation Results

In this section, we present and discuss the performance of our proposed algorithm. First, we provide some insight into the evolution of our trust estimates for two example nodes in a simulation run. Secondly, we evaluate the robustness of our algorithm to changes in simulation parameters such as number of friends, number of malicious nodes, and number of nodes. Finally, we compare our algorithm to an existing approach and demonstrate an improvement in performance.

Figure 1 presents the estimated trust values for a pair of randomly selected nodes in an extended 500-iteration-long simulation run. A well-behaved node and a malicious node are selected, both of which have an initial estimated trust value of 0.5. In Figure 1a, the estimated trust value for the well-behaved node exceeds the trustworthiness threshold (at 0.5) and stabilizes around 0.83, resulting in an accurately detected well-behaved node. Conversely, Figure 1b illustrates the estimated trust values for a malicious node engaging in bad-mouthing and ballot-stuffing attacks. The estimated trust value for this node drops below the threshold and settles at around 0.25, showing that the trust management model effectively identifies the malicious behaviour.

We have evaluated the performance of our proposed trust management approach following a fractional factorial design with three factors: total number of nodes ($N_U = N_V \in \{50, 75, 100, 150\}$), percentage of malicious nodes ($p_m \in \{0.1, 0.2, 0.3, 0.4\}$), and percentage of friends ($p_f \in \{10\%, 20\%, 30\%\}$) with 4, 4, and 3 levels respectively. We evaluate performance in terms of precision, recall, and F-score (Section V-B). These metrics measure the effectiveness of the trust management framework in detecting malicious nodes, when attackers provide false recommendations and randomly change their behaviour to deceive legitimate vehicles, as described in Section III-B. Each experimental unit (combination of simulation parameters) is simulated in batches of 100 runs (each started with a different seed), and the mean values of the three performance metrics are captured. The size of the simulated vehicular network area is $300m \times 300m$ in all simulations.

Table I shows a comparison of precision, recall, and F-score for different combinations of the percentage of friends and the total number of nodes. All results presented in the table were simulated with a fixed percentage of malicious nodes of 20%, which has been considered in recent works as an intermediate level for this parameter [1], [9]. Figure 2a is a graphical representation of the F-score results from Table I, both of which show that a higher number of nodes results in a better performance overall. This is due to the fact that a higher number of nodes implies a higher number of interactions between trustworthy nodes, resulting in more legitimate information circulating through the network. Furthermore, the figure shows that an increase in the percentage of friends also results in an overall increase in performance.

TABLE I: Effect of node density vs. number of friends

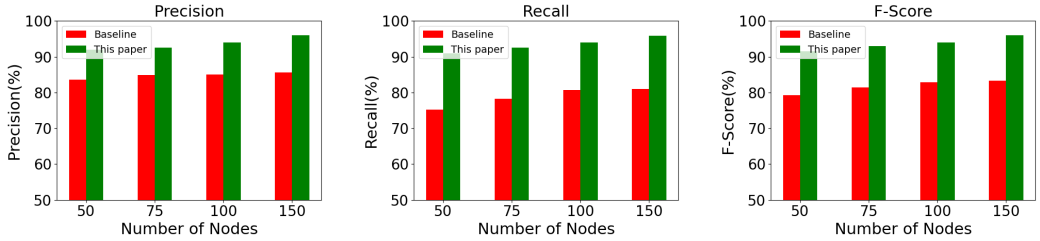
Number of Nodes	10% Friends			20% Friends			30% Friends		
	P	R	F	P	R	F	P	R	F
50	91.0	90.0	90.4	92.0	91.0	91.5	94.8	92.4	92.9
75	92.0	92.0	92.0	92.5	92.5	92.5	95.8	94.8	94.9
100	93.0	93.0	93.0	94.0	94.0	94.0	96.0	95.0	95.4
150	94.7	96.7	95.4	96.0	95.9	96.0	96.5	96.5	96.5

Table II shows a comparison of the three performance metrics for different combinations of number of nodes and percentage of malicious nodes. For these results, the percentage of friends was fixed at 20%. Table II corroborates the results of Figure 2a regarding node density, with higher performance associated with a higher number of nodes. Furthermore, an increase in the percentage of malicious nodes has a negative impact on the performance of the trust management algorithm. This is an expected result since an increase in the number of malicious nodes results in a larger volume of untrustworthy information being shared through the network, which is particularly harmful when it comes to indirect trust calculations.

TABLE II: Effect of node density vs. number of malicious nodes

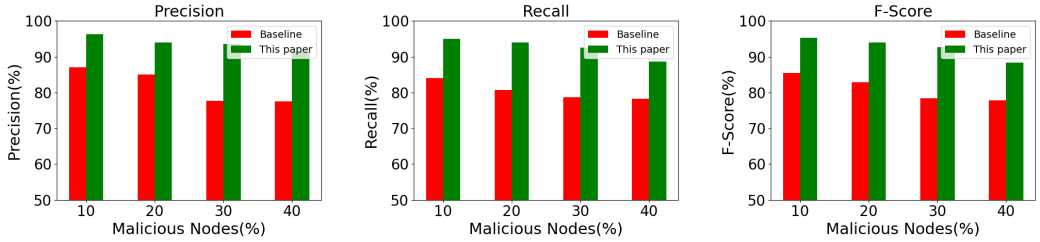
Malicious Nodes (%)	50 Nodes			100 Nodes			150 Nodes		
	P	R	F	P	R	F	P	R	F
10	94.3	93.4	93.2	96.2	95.	95.3	98.2	95.4	96.6
20	92.0	91.0	91.5	94.0	94.0	94.0	96.	95.9	96.0
30	89.0	89.0	89.0	93.5	92.5	92.7	96.5	95.0	95.7
40	82.8	88.1	81.4	91.4	88.7	88.5	94.0	94.7	94.0

Finally, Table III shows a comparison of performance for different percentages of malicious nodes and percentages of



(a) Precision (b) Recall (c) F-Score

Fig. 3: Comparison to baseline for different node densities (a) Precision (b) Recall (c) F-Score.



(a) Precision (b) Recall (c) F-Score

Fig. 4: Comparison to baseline for different percentages of malicious nodes (a) Precision (b) Recall (c) F-Score.

friends. Here, the total number of nodes in the network was fixed to 100. Figure 2b, a graphical representation of the F-score results from Table III, shows that an increase in the percentage of malicious nodes results in a decrease in the performance due to the increase of untrustworthy interactions. In this case, we can see that this is true regardless of the percentage of friends in the network. Furthermore, Table III corroborates the fact that a higher percentage of friends results in improved performance.

The effect of the *percentage of friends* on performance is a result of our proposed social trust calculations. In a network with a higher number of friends, nodes receive more recommendations that exhibit a higher level of social similarity. Consequently, these recommendations are given more weight in the computation of indirect trust. This process enriches the collection of second-hand observations, enhancing the overall robustness and reliability of indirect trust calculations.

TABLE III: Effect of number of friends vs. number of malicious nodes

Malicious Nodes (%)	10% Friends			20% Friends			30% Friends		
	P	R	F	P	R	F	P	R	F
10	96.3	96.8	96.3	96.2	95.0	95.3	97.0	97.0	97.0
20	93.0	93.0	93.0	94.0	94.0	94.0	96.0	95.0	95.4
30	92.5	92.2	92.3	93.5	92.5	92.7	94.5	94.5	94.5
40	92.2	89.6	89.5	91.4	88.7	88.5	93.0	93.0	93.0

Figures 3 and 4 show a comparison of precision, recall, and F-score between our proposed trust management framework and a baseline benchmark using the *weighted sum* method. This method was chosen due to its extensive use in numerous prior trust management schemes for wireless networks, such as [4], [5], [11]. Figure 3 shows a comparison of the performance metrics for different numbers of nodes. All results presented in the figure were simulated with a fixed percentage of malicious nodes of 20% and a fixed percentage of friends of 20%. Figure 3c illustrates that our trust management model consistently achieves higher precision scores compared to the baseline method as node density changes. Figure 4 shows the accuracy of the proposed trust model in terms of precision, recall, and F-score for different percentages of malicious nodes. For these results, the total number of nodes in the network was fixed to 100 and the percentage of friends was 20%. The figure shows that our proposed method also achieves higher accuracy compared to the baseline trust model for different percentages of malicious nodes.

VII. Conclusions

In this work, we have proposed a novel trust management model for the SIoV that uses the DST combination rule for indirect trust calculations, incorporating social similarities such as friendship, social contact, and community of interest, to weigh recommendations with different levels of importance. The preliminary evaluation of our model in detecting trustworthy nodes under common trust-related attacks shows performance similar to state-of-the-art methodologies across different simulation conditions, i.e., percentage of malicious nodes and overall number of nodes in the network. Furthermore, our trust management model also shows sensitivity to changes in the social relationships of the users. In the future, we plan to provide a more detailed analysis of the effect of other social similarity metrics on performance. Moreover, we will evaluate our trust model with more realistic vehicular mobility using the SUMO simulator.

REFERENCES

[1] Ahmad F, Kurugollu F, Kerrache CA, Sezer S, Liu L. NOTRINO: A NOvel Hybrid TRust Management Scheme for INternet-of-Vehicles. IEEE Transactions on Vehicular Technology. 2021 9;70:9244-57.

[2] Kerrache CA, Lagraa N, Hussain R, Ahmed SH, Benslimane A, Calafate CT, et al. TACASHI: Trust-Aware Communication Architecture for Social Internet of Vehicles. IEEE Internet of Things Journal. 2019 8;6:5870-7.

[3] Zhao Y, Liu W, Li B, Zhou X, Ning Z, Qiu T, et al. Entity and Sociality Trust-Aware Model for Content Distribution in Social Internet of Vehicles. IEEE Transactions on Vehicular Technology. 2022 12;71:12511-22.

[4] Xia H, Zhang SS, Li Y, Pan ZK, Peng X, Cheng XZ. An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology. 2019 7;68:7108-20.

[5] Alnasser A, Sun H, Jiang J. Recommendation-Based Trust Model for Vehicle-to-Everything (V2X). IEEE Internet of Things Journal. 2020 1;7:440-50.

[6] Raya M, Papadimitratos P, Gligor VD, Hubaux JP. On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks. I E E E; 2008. .

[7] Chen JM, Li TT, Panneerselvam J. TMEC: A Trust Management Based on Evidence Combination on Attack-Resistant and Collaborative Internet of Vehicles. IEEE Access. 2019;7:148913-22.

[8] Cui J, Zhang X, Zhong H, Ying Z, Liu L. RSMA: Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular Networks. IEEE Internet of Things Journal. 2019 8;6:6417-28.

[9] Li W, Song H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems. 2016 4;17:960-9.

[10] Cheng T, Liu G, Yang Q, Sun J. Trust Assessment in Vehicular Social Network Based on Three-Valued Subjective Logic. IEEE Transactions on Multimedia. 2019 3;21:652-63.

[11] Chen IR, Guo J, Bao F. Trust Management for SOA-Based IoT and Its Application to Service Composition. IEEE Transactions on Services Computing. 2016 5;9:482-95.

[12] Jøsang A, Hayward R, Pope S. Trust Network Analysis with Subjective Logic; 2006. Available from: http://www.crpit.com/Vol48.html.

[13] Jøsang A, Diaz J, Rifqi M. Cumulative and averaging fusion of beliefs. Information Fusion. 2010 4;11:192-200.

[14] Breese JS, Heckerman D, Kadie C. Empirical Analysis of Predictive Algorithms for Collaborative Filtering; 1998. .

[15] Society IC, of Electrical I, Engineers E. 2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON) : 21-25 June, 2010, Boston, Massachusetts. IEEE; 2010.